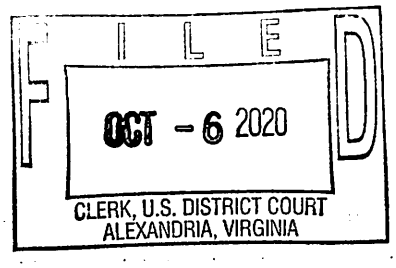
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:20cv1171 AJT/IDD

FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") and FS-ISAC, INC., ("FS-ISAC") hereby complain and allege that JOHN DOES 1-2 (collectively "Defendants"), have illegally created and are using for criminal purposes a global network of interconnected computers known as "Trickbot." Trickbot is comprised of computing devices connected to the Internet that Defendants have infected with malicious software (referred to as "malware"), including banking Trojans and distributing various malicious and deadly forms of ransomware. Defendants have used the Trickbot botnet through servers connected to the Internet to infect computers to steal millions of dollars. Unless enjoined and held accountable, Defendants will continue to use Trickbot to steal financial account information, funds, and personal information from millions of individuals as well as extort victims through the use of ransomware. Defendants control Trickbot through a command and control infrastructure ("Trickbot Command and Control Servers") hosted at and operating through the Internet Protocol addresses ("IP Addresses) set forth in **Appendix A**. Plaintiffs allege as follows:

NATURE OF THE ACTION

1. This is an action based upon: (1) the Copyright Act, 17 U.S.C. §§ 101 *eq seq.*; (2)

the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (3) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (4) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (5) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (6) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (7) Common Law Trespass to Chattels; (8) Unjust Enrichment; and (9) Conversion. Plaintiffs seek injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the Trickbot Command and Control Servers. Defendants, through their illegal activities involving Trickbot, have caused and continue to cause irreparable injury to Plaintiffs and their customers and members and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. Plaintiff FS-ISAC, Inc. is a non-profit corporation duly organized and existing under the laws of Delaware, having its headquarters and principal place of business in Reston, Virginia. FS-ISAC is a membership organization comprised of 4,400 organizations including global transaction banks, regional banks, and payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. FS-ISAC represents the interests of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry.

4. Defendant John Doe 1 controls the Trickbot Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A.**

5. Defendant John Doe 2 controls the Trickbot Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A.**

6. Defendants own, operate, control, and maintain the Trickbot botnet through a command and control infrastructure hosted at and/or operating at the IP Addresses set forth in **Appendix A**. The command and control infrastructure hosted and operated at the IP Addresses are maintained by the third-party hosting companies set forth at **Appendix A**. Plaintiffs will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Plaintiffs will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

7. Plaintiffs are informed and believe and thereupon allege that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that the injuries of Plaintiffs, their customers and members and the public, as herein alleged, were proximately caused by such Defendants.

8. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, aided and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of The Copyright Act (17 U.S.C. §§101 *et seq.*), The Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Plaintiffs' claims for trespass to chattels, conversion and unjust enrichment pursuant to 28 U.S.C. § 1367.

10. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a

substantial part of the events or omissions giving rise to Plaintiffs' claims has occurred in this judicial district, because a substantial part of the property that is the subject of Plaintiffs' claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants engage in conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein.

11. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing their activities, including theft of funds and information, at individual users located in the Eastern District of Virginia. Defendants have directed malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia. Defendants have attempted to and, in fact, have infected such user computers with malicious computer code. That code contains, without authorization, Microsoft's copyrighted computer code and instructions to Microsoft's Windows operating system, which compromises the security of those systems and steals sensitive information and funds from the individual users, all to the grievous harm and injury of Plaintiffs, their customers and members, and the public. **Figure 1**, below, depicts the geographic location of computing devices in the Eastern District of Virginia, against which Defendants are known to have directed malicious code through servers connected to the Internet, thereby enlisting them into the Trickbot botnet.

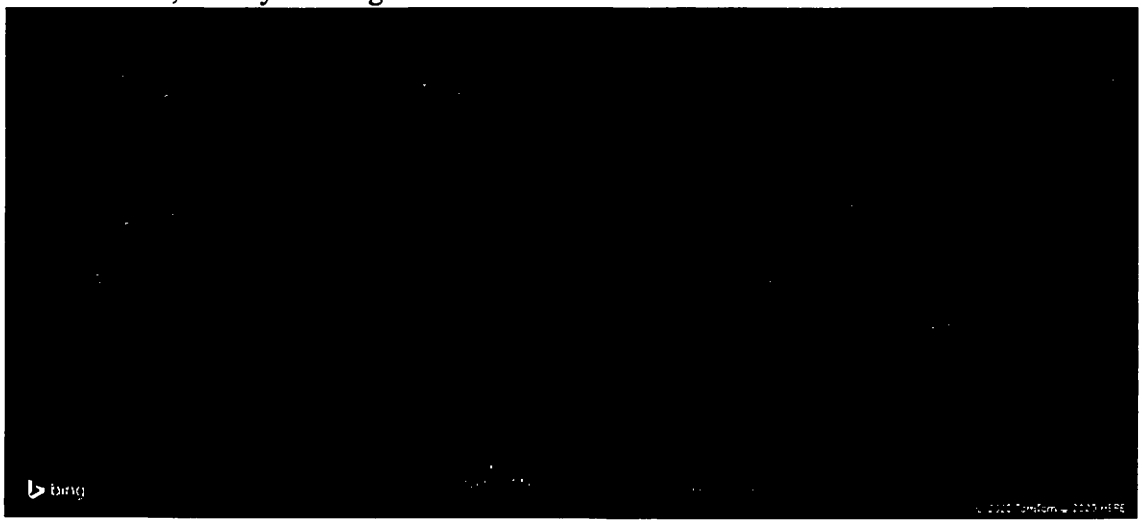


Figure 1

12. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A

substantial part of the events or omissions giving rise to Plaintiffs' claims, together with a substantial part of the property that is the subject of Plaintiffs' claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Plaintiffs' Services and Reputation

13. Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems. Microsoft® is a provider of the Windows® operating system, Outlook® email services and Microsoft Word®, Microsoft's word processing software. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft,® Windows,® Outlook,® and Word.® Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

14. One of the pillars of Microsoft's comprehensive portfolio of software programs is its Microsoft Windows operating system. Microsoft Windows is a group of proprietary graphical operating system families. Microsoft also spends considerable time and energy building its Windows platform and making it available to third-party developers to create programs that are compatible with Windows. With every Windows release, Microsoft also makes available a software development kit ("SDK"). The SDK is a package of programming tools including creative and original APIs, header files, libraries, documentation, code samples, processes, and guides that developers can use and integrate into their own applications. Microsoft's SDKs are required when developing any application, program, or tool for Microsoft Windows. The code at issue in this case encompasses a type of code called "declarations" within header files and within

libraries contained in the SDK, and referred to in this Complaint as the "Declaring Code."

15. Microsoft owns copyrights in the code, documentation, specifications, libraries, and other materials that comprise the Windows operating system, including the Declaring Code. Microsoft's Windows SDK copyrights, encompassing the Declaring Code, are registered with the United States Copyright Office, including those attached as **Appendix C**.

16. Microsoft makes its SDK and the code contained within the SDK, including the Declaring Code, available to the public through a license ("SDK License"). This enables Microsoft to maintain an open platform for third-party developers while preventing malicious actors from using the code in the SDK, including the Declaring Code, in a harmful way. Any developer who downloads Microsoft's SDK tools, including the Declaring Code, must accept the terms of the SDK License.

17. Microsoft's SDK License agreements make clear to end users that they are acquiring a license to use the software subject to certain limitations around the use of the software and place certain restrictions, including prohibiting end-users from using certain portions of the software code, including the header files in the SDK and associated Declaring Code, "in malicious, deceptive, or unlawful programs."

18. Plaintiff FS-ISAC is a trade organization comprised of 4,400 organizations including global transaction banks, regional banks, payment processors headquartered in North America, the European Union, and Asia-Pacific, and over 20 trade associations representing the majority of the U.S. financial services sector. It was established by the financial services sector in response to the 1998 Presidential Directive 63, later updated by the 2003 Homeland Security Presidential Directive 7, which requires that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the United States' critical infrastructure. Its purpose is "to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and interests...." FS-ISAC's activities include actively coordinating and promoting financial industry detection, analysis, and response to cyber security threats. Financial institutions that are members of FS-ISAC have generated substantial goodwill with their customers, establishing a strong brand and developing

their respective names and the names of their products and services into strong and famous world-wide symbols that are well-recognized within their channels of trade.

COMPUTER "BOTNETS"

19. A "botnet" is a collection of individual computers infected with malicious software ("malware") that allows communication among those computers and centralized or decentralized communication with other computers providing control instructions. A botnet network may be comprised of multiple, sometimes millions, of infected user computers. The individual computers in a botnet often belong to users who have unknowingly downloaded or been infected by malware. A user's computer, for example, may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads malware. In each instance, malware is downloaded or executed on the user's computer, causing that computer to become part of the botnet. Once part of a botnet, the user's computer is capable of sending and receiving communications, code, and instructions to or from other botnet computers.

20. Some botnets' computers are wholly within the control of the botnet creators. These may have specialized functions, such as sending control instructions to infected user computers. These are generally referred to as "command and control" computers.

21. Criminal organizations and individual cybercriminals often create, control, maintain, and propagate botnets in order to carry out misconduct that harms others' rights. They use botnets because of botnets' ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected user computer for a variety of illicit purposes, unknown to the end user. A computer in a botnet, for example, may be used to:

a. carry out theft of credentials and information, fraud, computer intrusions, or other misconduct;

b. anonymously send unsolicited bulk email without the knowledge or consent of the individual user who owns the compromised computer;

c. deliver further malware to infect other computers; or

d. "proxy" or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

22. Botnets provide a very efficient means of controlling a large number of computers and means of targeting any action internally against the contents of those computers or externally against any computer on the Internet.

OVERVIEW OF TRICKBOT

23. Trickbot is a prolific and globally diverse financial theft and malware distribution botnet. The Trickbot botnet is comprised of over a million infected end user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. Trickbot specializes in distributing ransomware, infecting end user computers in order to steal financial account credentials and funds, steal personal information or to install other forms of malware such as ransomware. The precise identities and locations of those behind the activity are generally unknown. Trickbot targets Plaintiffs' customers or member organizations, including end users who use Microsoft's operating system and online financial account infrastructure of FS-ISAC's financial services industry members.

24. Defendants use the Trickbot botnet primarily to gain access to account credentials for online banking websites to steal—among other things—funds from computer users and financial institutions. When a user of a Trickbot-infected computer attempts to log onto a financial institutions website, Trickbot (a) secretly hijacks the user's web browser, (b) captures the user's online financial login credentials and other personal identifying information, and (c) sends that information to Defendants. The user is unaware of Trickbot's activity as Defendants have designed Trickbot to hide itself and its unlawful activity on infected computers. After Trickbot captures the user's login credentials and personal identifying information, Defendants use that information, for example, to access the user's bank account. The user perceives only a normal login and is unaware of Defendants' surveillance and control of their computer and theft of their identity and of funds from their account.

TRICKBOT'S COMMAND AND CONTROL SERVERS

25. After Trickbot infects a victim computing device, it connects over the Internet to one of its pre-programmed command and control servers. In its first communication, it sends the command and control server the victim computer's IP address, the version of Windows running on the computer, a unique computing device identifier and a machine language identifier. At this point, it is ready to begin executing commands sent to it by the Defendant botnet operators.

26. The primary command and control communications channel between infected victim computers and Defendants' command and control computers is comprised of particular IP addresses associated with servers directly controlled by Defendants, reflected in **Appendix A**. This is referred to as the "Trickbot Command and Control Servers." An IP address can be thought of as the physical location on the Internet of a particular computer. An "IP address" is a unique string of numbers separated by a period, such as "149.154.152.161" that identifies each computer attached to the Internet. Defendants must lease such computers from companies that provide "hosting" services, and which assign to those computers particular IP addresses. The hosting company refers to a type of company that specializes in offering computer hardware, software, connection to the Internet, technical support, and other services to companies and individuals seeking to have some presence on the Internet.

27. **Figure 1** reflects the relationship between the Trickbot Command and Control Servers and infected computers:

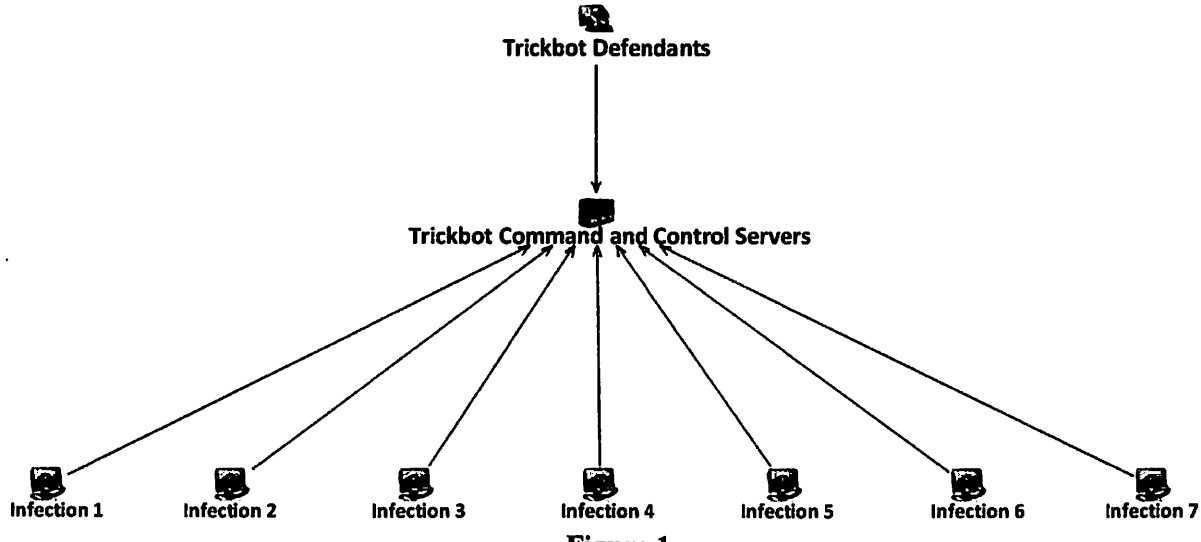


Figure 1

TRICKBOT'S INITIAL INFECTION OF VICTIM DEVICES

28. Defendants use various means of infecting end-user computers. Trickbot arrives into a victim's system either by being delivered through malicious links or attachments in spam email or delivery through other forms of malware. Defendants conduct spam email campaigns, involving unsolicited emails that direct users to download the Trickbot malware from malicious websites or trick the user into opening malicious attachments, masquerading as Microsoft Word documents. The following **Figure 2** shows a deceptive phishing email leveraging Microsoft's Word trademark and deceiving the user through use of a fraudulent "tax" related theme.

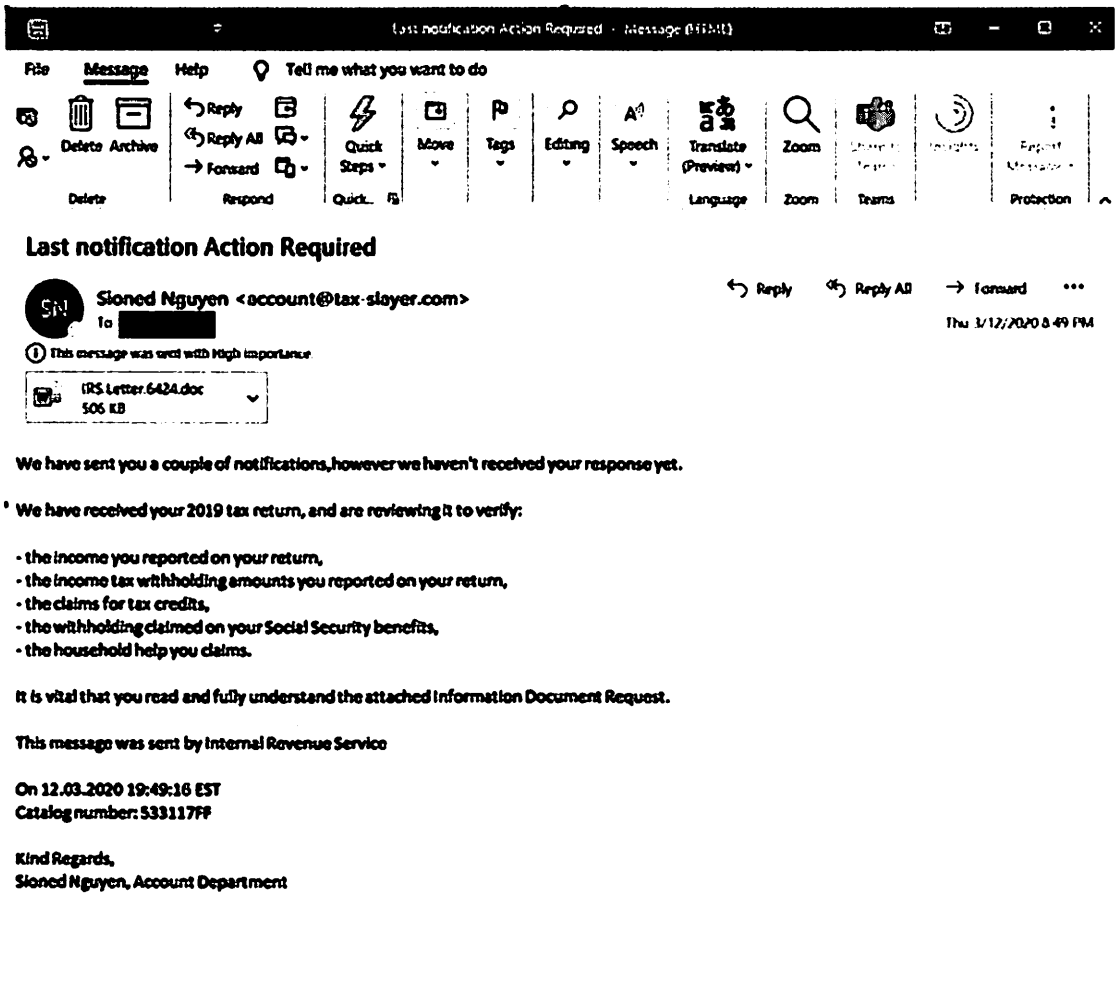


Figure 2

29. Once on a system, Trickbot utilizes its rootkit capabilities to disable a large number of security applications, among them Windows Defender, both to protect itself and other malware on the infected system.

30. The user of the infected computer is unaware of Trickbot's activity as Defendants have designed Trickbot to hide itself and its unlawful activity on infected computing devices in part by disabling the security defenses of the user's device. The operating system still purports to be Windows, but, in fact, Trickbot has corrupted and thereby converted the Windows operating system into instruments of fraud aimed directly at the user of the computing device. The typical user is unaware of Defendants intrusion, theft, surveillance and control of their computing device.

31. In addition to targeting user's credentials, the Defendants also utilize malware – the most common being indigenous implants named "Ryuk," "CobaltStrike," and "Mimikatz" – to compromise systems, distribute ransomware, and steal data from victim systems. The Defendants use Microsoft's trademarks to cause victims to download attachments appearing to be legitimate, including for example Microsoft Word attachments, but which result in installation of this malware on the victims' computers. Once installed on a victim's computer, this malware exfiltrates information from the victim computer, maintains a persistent presence on the victim computer, and waits for further instructions from the Trickbot defendants.

32. During Trickbot's initial infection on the victim computer, the infected device will run the malware's executable file, creating a folder inside the *%APPDATA%* local user folder. The malware will then change a number of settings in the user's Windows scheduled tasks. Trickbot achieves this by writing entries to Windows registry and folder paths, modifies the system processes that contain the "Microsoft" and "Windows" trademarks. The following are examples of such Trickbot registry paths:

- *%WINDIR%\System32\Tasks\, for example Ex: C:\Windows\System32\Tasks*
- *%WINDIR%\Tasks\, for example C:\Windows\Tasks*
- *HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache\Tasks*
- *HKLM\SOFTWARE\Policies\Microsoft\Windows Defender*
    - *DisableAntiSpyware*

- *HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection*
    - *DisableBehaviorMonitoring*
    - *DisableOnAccessProtection*
    - *DisableScanOnRealtimeEnable*
    - *DisableIOAVProtection*

33. From there, details and information from the victim computer are saved to victim's computer and sent to one of the command and control servers of the Trickbot defendants, who then send additional instructions and commands to the victim's computer, and can exfiltrate additional stolen information from that computer. By specifically targeting Microsoft's Windows operating system and utilizing registry and file paths containing Microsoft's trademarks, in order to deceive users and carry out the fraudulent scheme, the Trickbot defendants infringe Microsoft's trademarks and deceptively use those trademarks in the context of Microsoft's Windows operating system.

TRICKBOT'S LITERAL COPYING OF MICROSOFT'S COPYRIGHTS

34. Trickbot is an active, sophisticated, and modular botnet, which enables its operators to easily add or remove capabilities. Once this initial infection period is complete, the infected device will start to communicate with the Trickbot Command and Control Servers to download additional malware modules. These secondary malware infections make further changes to the computer device, including by adding files, changing registry settings, opening additional backdoors that allow remote control by other cybercriminals, altering the integrity of certain software contained in Windows, such as Internet Explorer, Edge, or Outlook, and allowing further sets of malwares to be downloaded onto the computing device.

35. Depending on the intention of Trickbot's operators for a particular intrusion, Trickbot can download and deploy from the Trickbot Command and Control Servers various modules that provide varying forms of functionality and criminal activity, as shown in **Figure 3**. Trickbot contains several reconnaissance modules that were updated precisely for the function of going back and evaluating whether a system is worthy of revictimization with ransomware. Once a victim system is identified as a potential target for ransomware, the Trickbot Defendants will

deploy an additional payload that carries out additional reconnaissance functionality (using tools such as CobaltStrike and Mimikatz) and finally deploys the Ryuk ransomware on the victim system. The modules are sent with a configuration file. Our investigation has seen Trickbot modules—also referred to as secondary malware infections—with the following names and purposes:

Figure 3

Module	Purpose
injectDll	Main banker module using "static" and "dynamic" web browser injection and data theft
networkDll	A reconnaissance module that gathers network and system information for the purpose, among many, to determine if the victim machine meets criteria for revictimization with ransomware
Systeminfo	Gathers system information
tabDll	Propagate Trickbot via EternalRomance Exploit
wormDll	Propagate Trickbot via SMB - EternalBlue Exploit
shareDll	Propagate Trickbot via Windows Network Shares
vncDll / BCTestDll	Remote control/Virtual Network Computing module to provide backdoor for further module downloads
rdpscanDll	Launch brute-force attacks against selected Windows systems running a Remote Desktop Protocol (RDP) connection exposed to the Internet
mailsearcher	Searches all files on disk and compares their extensions to a predefined list to harvest email addresses
outlookDll	Gather Outlook credentials
importDll	Gather browser data
psfin	Gather point of sale software credentials
squlDll	Gather email addresses stored in SQL servers
aDll	Execute various commands on a Windows domain controller to steal Windows Active Directory Credentials
pwgrab	Gather credentials, autofill data, history and so on from browsers

36. Each module has a configuration file containing code required to enable the module to interact with the Windows operating system to perform their malicious tasks. The configuration codes are hosted at IP addresses associated with Trickbot's Command and Control

Servers. Once activated, modules will connect over the Internet to the Command and Control Servers to load the configuration codes the module requires to perform its malicious tasks.

37. The configuration codes contain literal verbatim copying of the code expressions, organizations, and hierarchies of hundreds of lines of Declaring Code from Microsoft's SDK. Thus, each malicious malware module contains literal copying of the Declaring Code.

38. The Trickbot authors' voluminous, unauthorized, and illegal misappropriation of the Declaring Code has been crucial to Trickbot's attempts to infiltrate victim devices and steal financial information. In this way, the Trickbot authors are using without authorization Microsoft's own copyrighted Declaring Code in order to target and attack any computing device running Microsoft Windows operating system, infiltrate Windows' functionalities, and alter the integrity of certain software contained in Windows.

39. For example, within the malicious Trickbot "injectDll" file, the Defendants copied literal code and the structure sequence and organization of Windows code such as the AdjustTokenPrivileges, TerminateThread, LookupPrivilegeValueW, RevertToSelf, DuplicateTokenEx, OpenProcessToken, LoadLibrary, GetProcAddress, GetCurrentProcess, CloseHandle code and many other Windows code elements. The following is a representative example of such literally infringed source code:

```
// declaration of function pointer for advapi32.dll
typedef BOOL (*AdjustTokenPrivileges)(
    HANDLE              TokenHandle,
    BOOL                DisableAllPrivileges,
    PTOKEN_PRIVILEGES NewState,
    DWORD               BufferLength,
    PTOKEN_PRIVILEGES PreviousState,
    PDWORD              ReturnLength
    );
```

40. The following chart includes a few representative examples of the hundreds of lines of Microsoft's Declaring Code and the structure, sequence, and organization of that code that are copied within and across the numerous Trickbot modules:

Figure 4

HARM TO PLAINTIFFS AND THEIR CUSTOMERS, MEMBER ORGANIZATIONS, AND THE PUBLIC

41. Defendants inflict severe harm on individuals whose computing devices is infected with the Trickbot malware. Once a computing device is infected with Trickbot, Defendants can use the victim's computer to steal the victim's online banking credentials and funds from their online financial accounts, constantly monitor their online activities, send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. Defendants' primary goal, as made evident by the Trickbot functionality, is to deliver financial theft malware, deliver ransomware, enable attacks against other computers and to steal online account login IDs, passwords, and other personal identifying information.

42. A Trickbot attack begins when Trickbot detects the user's attempt to connect to a financial institution's website. When this occurs, Trickbot can proceed in several ways. Trickbot can, for example, engage in a "web-inject"[1] attack, sometimes also referred to as a "man-in-the-browser" attack, monitors the victim's activity and detects when the victim is navigating via their browser to the online portals of a wide variety of financial institutions, including global

[1] A web inject is code that manipulates the appearance of a website, such as an online banking website, before it is rendered on the web browser. This has the effect of modifying rendered website content to achieve any number of goals the malicious actor chooses, such as adding, removing, or modifying text, inserting new or different form fields requesting personal or security information to deceive the user, and capturing such data entered by the victim into fields.

transaction banks, regional banks, and payment processors. When the module detects that the user is visiting such a website, it utilizes the web inject method to either send the user to a fake website that mimics the financial institution or to alter or replace content or display additional fields in the website as it appears to the victim in their browser. In this way, the victim believes that they are at the legitimate online financial website, when in fact they are seeing either an entirely fake version of the website to which the Trickbot module has diverted them, or a version of the website that has been manipulated by Defendants.

43. Regardless which method is used the effect is the same. When the user types their login credentials into the website or types additional information into fraudulent fields injected by the Defendants (such as pin codes, answers to security questions or other personal information), the Defendants are able to intercept that information and use it to log into the user's online accounts. The Defendants can then initiate funds transfers, resulting in theft of the victim's money. This process is reflected in **Figure 5** is but one example of a web inject targeting a particular financial institution among hundreds globally.

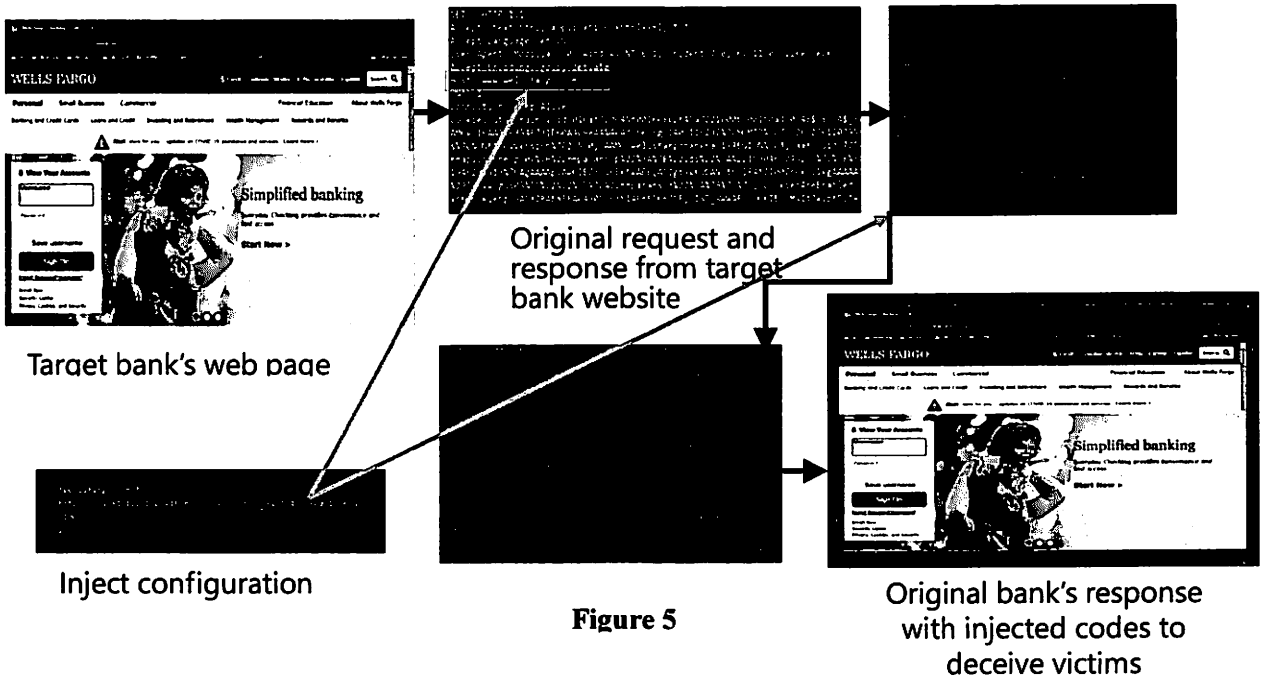


Figure 5

44. The Trickbot malware infection further harms Plaintiffs' customers, member

organizations, and the public by damaging the end user computing devices and the software installed on those devices licensed from Microsoft, including degrading the integrity of the computers and the operating system, intruding into those devices, disabling some of those systems' antivirus software, and carrying out malicious actions from those computers and directed toward the owners of those computers. During the infection of a user's device, the Trickbot malware makes changes at the deepest and most sensitive levels of the device's operating system. Additionally, it makes fundamental changes at the level of the Windows registry. Microsoft's customers whose computing devices are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and function of the user's operating system, destabilize it, and forcibly draft the customers' devices into the botnet.

45. Trickbot severely damages the computing devices it infects, making low-level changes to the operating system and disabling the primary security defense of most computing devices by blocking the computing device from getting anti-virus software updates. In fact, Trickbot is specifically designed to disable known antivirus products, including Windows Defender, Sophos, and Malwarebytes, that would otherwise protect devices from the Trickbot malware. As one example, Trickbot is designed to target Windows Defender by attacking the Registry settings and performing the following steps:

a. Disable and then delete the WinDefend service.
b. Terminates the MsMpEng.exe, MSASCuiL.exe, and MSASCui.exe processes.
c. Adds the DisableAntiSpyware Windows policy and sets it to true to disable Windows Defender and possibly other software.
d. Disables Windows Security notifications.
e. Disables Windows Defender real-time protection.

46. As a result, Trickbot not only cripples the security mechanism that might result in removal of Trickbot from the computing device, it may leave victim's computing devices exposed to against many other types of malware.

47. Once a computing device is infected, the Windows operating system cease to operate normally and are transformed into tools of deception and theft. But Windows still bears Microsoft's trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. Trademark registrations for the

marks infringed by Defendants are attached to this complaint as **Appendix B.**

48. Customers who experience degraded performance of Microsoft's product may attribute such poor performance to Microsoft, causing extreme damage to Microsoft's brands and trademarks and goodwill associated there with. Even customers who eventually come to learn their computing devices are infected with malware may incorrectly attribute the infection to vulnerabilities in Microsoft's products, because many customers are unaware that they have fallen prey to Defendants' attacks.

49. Moreover, as a provider of Windows, Microsoft devotes significant computing and human resources to combating Trickbot and other malware infections and helping customers determine whether or not their computing devices are infected and, if so, cleaning them. Not only does Microsoft expend resources in helping users combat Trickbot, these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. Microsoft, as a provider of the Windows operating systems, must also incorporate security features in an attempt to stop installation of the Trickbot malware and other malicious software that is distributed by the Trickbot botnet. Microsoft has expended significant resources to investigate and track the Trickbot Defendants' illegal activities and to counter and remediate the damage caused by the Trickbot botnet to Microsoft, its customers, and the general public.

50. The Trickbot malware is designed to enable other criminal actors to transmit additional types of malware to infect end user computing devices. Each of the malware module infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal botnet infrastructure beyond Trickbot receiving additional commands.

51. One method Trickbot uses to infect victim devices is phishing emails. FS-ISAC members have reported Trickbot malware and phishing related attacks in the thousands just in

September 2020 alone. Trickbot attempted to steal over $7 million from FS-ISAC members. The average amount Trickbot attempted to steal in each attack was over $268,000.

52. Trickbot is also designed to download and spread secondary malware onto Trickbot-infected computers. For example, Trickbot can also distribute malicious code such as CobaltStrike and Mimikatz, which enable ransomware deployment, movement within victim systems and extraction of victim credentials. Trickbot infects a victim's system by being downloaded by other malware, such as the malware called "Emotet," or being delivered through spammed email attachments or malicious advertisements. Also, as indicated above, once installed, Trickbot can propagate itself throughout a network using the EternalRomance and EternalBlue exploits, or by means of Windows Network Shares.

53. One form of malicious code Trickbot delivers is ransomware. Ransomware is a form of malware designed to prevent victims from accessing their systems or personal files and demands ransom payment in order to regain access. Ransomware can have devastating effects. On information and belief, a recent Trickbot-associated ransomware attack on a German hospital crippled its IT network and contributed to the death of a woman who was unable to obtain emergency treatment. Ransomware has even been cited by the Department of Homeland Security as having the potential to disrupt infrastructure that will be used in the 2020 election. Further, on information and belief, ransomware was recently credited for attacking a company that sells software that cities and states use to display results on election night.

54. Trickbot distributes the Ryuk crypto-ransomware, a form of ransomware that encrypts a victim user's files, folders, and hard-drives and demands a ransom in Bitcoin or other cryptocurrency to retrieve the data. Ryuk is a sophisticated crypto-ransomware because it identifies and encrypts network files and disables certain Windows functionalities that prevent the user from being able to recover from the attack without external backups. On information and belief, Ryuk has been credited with attacking organizations, including municipal governments, state courts, hospitals, nursing homes, enterprises, defense contractors and large universities.

55. To carry out the intrusion into computing devices, Defendants cause the Trickbot malware to make repeated copies of Microsoft's trademarks onto computing devices, in the form

of file names, target names, and/or registry paths containing the trademarks "Microsoft" and "Windows." These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not.

56. Similarly, in creating deceptive versions of financial institution web pages, the Defendants make and use counterfeit copies of the trademarks of financial institutions that are FS-ISAC members, including but not limited to the trade names of such financial institutions and the trademark logos of these institutions. Defendants use those counterfeit trademarks to deceive consumers and to carry out schemes enabling the theft of online banking credentials. This activity causes injury to the FS-ISAC member institutions, by diminishing their brands and goodwill. This activity causes injury to the FS-ISAC member institutions and their customers by causing confusion to consumers and victims of such schemes by leading them to believe that the counterfeit trademarks and webpages created by the Trickbot botnet originate from the legitimate brand owner when, in fact, Trickbot alters them in a way that facilitates account fraud.

FIRST CLAIM FOR RELIEF

COPYRIGHT INFRINGEMENT, 17 U.S.C. §§ 101 *et seq.*

57. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 56 above.

58. Microsoft owns copyrights in the code, documentation, specifications, libraries, and other materials that comprise the Windows system and the associated SDK.

59. By Defendants' actions alleged above, Defendants have infringed and will continue to infringe, the Declaring Code by, *inter alia*, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from, substantially similar to and derived from the Declaring Code, in violation of Microsoft's exclusive rights at least under 17 U.S.C. § 101 *et seq*. without any authorization or other permission from Microsoft.

60. Defendants have reproduced and distributed the Trickbot code containing Microsoft's Declaring Code on devices leased from hosting companies that provide "hosting

services," which assign to those devices particular IP addresses to have a presence on the Internet. Defendants use the hosting services to transmit the malicious software through the Internet to the victims. Such use is not authorized. Defendants have thus induced, caused, and materially contributed to the infringing acts of others by inducing, allowing, and assisting others to copy and distribute the infringing code.

61. Defendants' infringement of Microsoft's copyrights has been deliberate, willful, and in utter disregard of Microsoft's rights.

62. Defendants have realized unjust profits, gain, and advantages as a proximate result of their infringement.

63. Defendants will continue to realize unjust profits, gain, and advantages as a proximate result of their infringement as long as such infringement is permitted to continue.

64. As a direct and proximate result of Defendants' willful copyright infringement, Microsoft has suffered, and will continue to suffer, monetary loss to its business, reputation, and goodwill. Microsoft is entitled to recover from Defendants, in amounts to be determined at trial, the damages it has sustained and will sustain, and any gains, profits, and advantages obtained by Defendants as a result of Defendants' acts of infringement and use and publication of copied materials.

65. Microsoft is entitled to an injunction restraining Defendants from engaging in any further such acts in violation of the United States copyright laws. Unless Defendants are enjoined and prohibited from infringing Microsoft's copyrights, inducing others to infringe Microsoft's copyrights, and unless all infringing products and advertising materials are seized, Defendants will continue to intentionally infringe and induce infringement of Microsoft's registered copyrights.

SECOND CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

66. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 65 above.

67. Defendants knowingly and intentionally accessed and continue to access protected

computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

68. Defendants' conduct involved interstate and/or foreign communications.

69. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

70. Plaintiffs seek injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

71. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

72. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 71 above.

73. Microsoft's Windows operating system software, and Microsoft's customers' computers running such software, and the online financial account infrastructure of FS-ISAC's member financial institutions are facilities through which electronic communication service is provided to users and customers.

74. Defendants knowingly and intentionally accessed the Windows operating system and FS-ISAC's members' online financial account infrastructure, and associated software, services and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft or FS-ISAC's members.

75. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users and FS-ISAC's members and their users.

76. Plaintiffs seek injunctive relief and compensatory and punitive damages in an

amount to be proven at trial.

77. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FOURTH CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et seq.*

78. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 77 above.

79. Defendants have used Microsoft's and FS-ISAC's member institutions' trademarks in interstate commerce.

80. The Trickbot botnets generate and use unauthorized copies of Microsoft's trademarks in fake and unauthorized versions of the Windows® operating system, Outlook®, and Word® software and content, including through the software operating from and through the Trickbot Command and Control Servers, as well as using Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft®, Windows®, Outlook®, and Word®, among other trademarks. The Trickbot botnets also generate and use unauthorized copies of FS-ISAC member institutions' trademarks. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and software and fake and unauthorized online financial account login webpages.

81. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act.

82. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

83. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

84. Defendants' wrongful and unauthorized use of Plaintiffs' trademarks to promote,

market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

FIFTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

85. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 84 above.

86. Microsoft's and FS-ISAC member institutions' trademarks are distinctive marks that are associated with Microsoft and FS-ISAC's member institutions and exclusively identify their businesses, products, and services.

87. Defendants make unauthorized use of Microsoft's and FS-ISAC's member institutions' trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products and FS-ISAC member institution services that are likely to cause confusion, mistake, or deception.

88. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act, 15 U.S.C. § 1125(a).

89. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

90. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

91. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 90 above.

92. Microsoft's and FS-ISAC's member institutions' trademarks are famous marks that are associated with Microsoft and FS-ISAC's member institutions and exclusively identify their businesses, products, and services.

93. Defendants make unauthorized use of Microsoft's and FS-ISAC's member

institutions' trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Plaintiffs' trademarks.

94. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

95. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

96. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 95 above.

97. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

98. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers and of FS-ISAC's member institutions.

99. Defendants' actions in operating Trickbot result in unauthorized access to Microsoft's Windows operating system software and the computers on which such programs run, as well as unauthorized access to the online financial account infrastructure of FS-ISAC's member institutions, and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds.

100. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

101. Defendants' actions have caused injury to Microsoft and its customers and to FS-ISAC's member institutions, and have interfered with the possessory interests of Microsoft over its software and with the FS-ISAC's member institutions' possessory interests in their respective computers and computer networks.

102. Plaintiffs' seek injunctive relief and compensatory and punitive damages in an

amount to be proven at trial.

103. As a direct result of Defendants' actions, Plaintiffs have suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Unjust Enrichment

104. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 103 above.

105. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft and FS-ISAC's member institutions in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft and online account infrastructure belonging to FS-ISAC's member institutions to facilitate unlawful conduct inuring to the benefit of Defendants.

106. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's and FS-ISAC's member institutions' property.

107. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of that property.

108. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

109. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

110. As a direct result of Defendants' actions, Plaintiffs and FS-ISAC's member institutions suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

NINTH CLAIM FOR RELIEF

Conversion

111. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs

1 through 110 above.

112. Microsoft owns all right, title, and interest in its Windows operating system software. FS-ISAC's member institutions own all right, title and interest in their online financial account infrastructure. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows operating system software and dispossessed FS-ISAC's member institutions of control over their online financial account infrastructure.

113. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

114. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

115. Defendants have converted funds from FS-ISAC member institutions through unauthorized withdrawals of funds from customer accounts using stolen online banking credentials.

116. Plaintiffs seek injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

117. As a direct result of Defendants' actions, Plaintiffs and their customers and member institutions suffered and continue to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays that the Court:

A. Enter judgment in favor of Microsoft and against the Defendants;

B. Declare that Defendants have infringed Microsoft's copyrights;

C. Declare the substantial likelihood that Defendants will continue to infringe Plaintiffs' intellectual property unless enjoined from doing so;

D. Declare that Defendants' conduct has been willful and that Defendants have acted

with fraud, malice and oppression;

E. An order that all copies made or used in violation of Microsoft's copyrights and Plaintiffs' trademarks, and all means by which such copies may be reproduced, be impounded and destroyed or otherwise reasonably disposed of;

F. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

G. Enter a preliminary and permanent injunction giving Microsoft control over the IP addresses used by Defendants to cause injury and enjoining Defendants from using such instrumentalities;

H. Enter judgment awarding Plaintiffs actual damages from Defendants adequate to compensate Plaintiffs for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

I. Enter judgment disgorging Defendants' profits;

J. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial;

K. Enter judgment awarding attorneys' fees and costs; and

L. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: October 6, 2020

Respectfully submitted,

/s/ Julia R. Milewski

Julie Rebecca Milewski (VA Bar No. 82426)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com

Gabriel M. Ramsey (*pro hac vice* pending)
Kayvan M. Ghaffari (*pro hac vice* pending)
Jacob Canter (*pro hac vice* pending)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Richard Domingues Boscovich (*pro hac vice* pending)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.